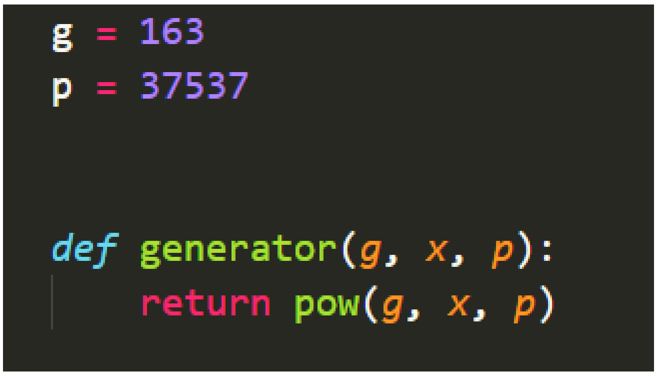
Diffie-Hellman



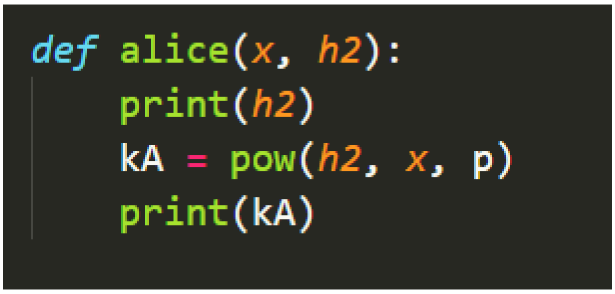
```python
g = 163
p = 37537


def generator(g, x, p):
    return pow(g, x, p)
```

G = Generator of the cyclic group 37537

P = Order of the group

Generator()

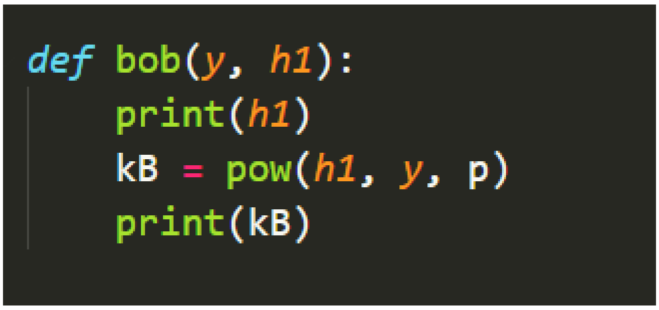
Takes g,x, and p as input, return g^x mod p to the calling function.



```python
def alice(x, h2):
    print(h2)
    kA = pow(h2, x, p)
    print(kA)
```

Alice()

Alice already has x and gets h2 which is g^y from Bob. Alice computes kA from the parameters and she gets the key.



```
def bob(y, h1):
    print(h1)
    kB = pow(h1, y, p)
    print(kB)
```

Bob()

Similar to Alice, Bob has y already and receives h1 from Alice, where h1 = g^x. He computes kB and gets the full key.

Sample Input

X: 1231

Y: 2312

Sample Output

Key: 19431